AIR WAR COLLEGE

AIR UNIVERSITY

AIRMEN AS BOLD RISK TAKERS

REDEFINING RISK TO ACHIEVE OPERATIONAL AGILITY

by

Jonathan E. Zall, Lieutenant Colonel, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Frank D. Samuelson, Colonel, USAF

15 April 2017

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lt Col Zall is assigned to the Air War College, Air University, Maxwell AFB, AL. He earned his commission through the Reserve Officer Training Corps program at the University of Illinois in Champaign-Urbana. Lt Col Zall is a senior Air Battle Manager and has served as a Combat Air Advisor in Iraq. He is a graduate of the U.S. Air Force Weapons School and the Air Force Institute of Technology at Wright-Patterson Air Force Base in Ohio.

Abstract

The Air Force Future Operating Concept identifies the goal to achieve "Operational Agility", which is necessary for success in future combat against near-peer adversaries. In order for the U.S. Air Force to reach the goal of Operational Agility, as stated in the Air Force Future Operating Concept, the Joint Doctrine definition of risk must change, and the Air Force must adopt a bolder approach to risk, because current definitions conflate risk with hazards, and Air Force "Risk Management" measures, at best, hedge risk while ignoring the necessity to exploit risk. The International Standards Organization has adopted a generalized definition of risk that incorporates both up-side and down-side aspects of risk. Aswath Damodaran and Michael Mauboussin provide insights for understanding risk and its relationship with uncertainty and luck, and for approaching risk from a positive, risk-exploitation orientation. A new definition and positive, disciplined approach to risk will empower Airmen leaders at all levels to effectively articulate and, in turn, comprehended Commander's Intent, and thereby to distribute control, decentralize execution, and seize the initiative at the lowest possible levels. Moreover, without a bolder approach to risk, Airmen will miss opportunities for initiative and innovation critical in future multi-domain, anti-access and area denial operations. To succeed in those future battlespaces, the Air Force must develop and entrust Airmen leaders to exploit risk instead of fearing or completely avoiding risk, because the ability to discover and capitalize on unplanned but advantageous opportunities will be the decisive factor in future near-peer military conflict.

"Fortune favors the bold"
– Latin Proverb

Introduction

What is risk? Is it potential danger? Or is it a calculated gamble? U.S. Air Force and joint guidance documents use the word "risk" interchangeably with other concepts, including "chance", "threat", and "possibility". Such imprecision is surprising, considering the Joint Operation Planning Process (JOPP) elevates "risk" to be on par with the other fundamental elements of strategy: ends, ways, and means.[2] In addition to conflating terms, the Joint Publication 1-02 definition of risk ("Probability and severity of loss linked to hazards")[3] is problematic in that it instills a negative orientation toward risk, and it obscures the relationship between risk and uncertainty. In his 2004 article on defining risk, Glyn Holton prompts his readers to consider the risk incurred by someone jumping out of an airplane with no parachute.[4] Current doctrine would label that as an act of extreme risk: the severity of loss is absolute (death), and it is certain to happen (probability = 1). However, Holton contends that, while leaping without a parachute is extremely—or maximally—hazardous, the doomed jumper faces no *risk* at all. The reason is that risk is inextricably tied to uncertainty, and there is no uncertainty in the outcome of the ill-equipped skydiver's course of action.[5]

Building on Holton's argument, Aswath Damodaran, in his 2007 book *Strategic Risk Taking: A Framework for Risk Management*, asserts both negative and positive outcomes are intrinsic to risk. Risk Management (RM) programs, as directed by Joint and Air Force guidance, are based on the joint definition of risk which only admits of negative events and outcomes (hazards and loss). The result is a negative approach, wherein commanders must continuously attempt to minimize risk, if not eliminate it entirely. The problem with a negatively-oriented

approach to risk, as Damodaran points out, is that reducing the down-side of risk unavoidably diminishes the up-side (positive outcomes) as well: actions that minimize risk also minimize opportunity.[6] While Joint and Air Force RM processes focus almost exclusively on risk reduction, the Army Doctrine Publication 6-0 "Mission Command" concept at least acknowledges the link between risk and opportunity.[7] In its goal to enable decentralized execution, the Mission Command concept affirms the necessity, in certain circumstances, to accept "prudent risk" in order to capitalize on available opportunities and thereby seize initiative.

In future combat scenarios, capitalizing on unplanned opportunities may be more than occasionally serendipitous; it may be the decisive factor between victory and defeat, especially against a near-peer adversary. In his 2012 book, *The Success Equation*, Michael Mauboussin describes the "Paradox of Skill": over time as the average skill-level exhibited by participants in a particular endeavor increases, the variance in skill between the top performers tends to narrow.[8] When this occurs, luck—that which cannot be controlled or affected by skill—becomes dominant over a marginal edge in skill for determining outcomes. Figure 1 illustrates this phenomenon.[9] The Skill Paradox indicates that as near-peer competitor warfighting skills approach parity with U.S. capabilities, Americans' marginal advantage will be less decisive than luck. Put another way, Airmen cannot control luck, but they can increase their exposure to it and capitalize on it, and therefore the ability to increase the availability of, discover, and exploit unplanned opportunities will be pivotal in future near-peer military conflicts.

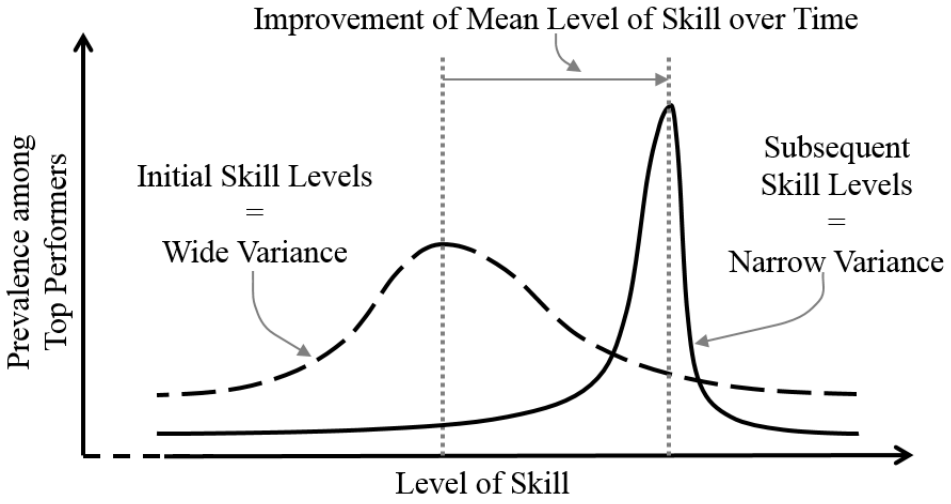

Figure 1. The "Paradox of Skill": Change in distribution of skill sets as overall expertise increases

Combining insights from Damodaran and Mauboussin for application in near-peer contested battlespaces, Air Force leaders must seek out and exploit risk in order to increase the availability—in terms of number, type, and magnitude—of opportunities which are the manifestations of luck. Waiting until that future fight occurs to impel rational risk-seeking attitudes in leaders is a recipe for defeat. The Air Force must start now to inculcate a bolder approach to risk in leaders so that disciplined risk-exploiting practices and mindsets are second-nature when advanced technologies and skills fail to deliver decisive advantages. Industry has already moved away from limiting risk approaches to minimizing negative outcomes. The International Standards Organization (ISO) defines risk as "effect of uncertainty on objectives", which opens up the possibility for both "up-side" and "down-side" risk.[10] With this new definition, the U.S. Air Force can begin to instill a positive, disciplined approach to risk; one that maximizes the availability of decisive opportunities in future operations.

Thesis

In order for the U.S. Air Force to reach the goal of Operational Agility, as stated in the Air Force Future Operating Concept[11], the Joint Doctrine definition of risk must change, and the Air Force must adopt a bolder approach to risk, because current definitions conflate risk with hazards, and Air Force RM measures, at best, hedge risk while ignoring the necessity to exploit risk. A new definition and positive, disciplined approach to risk will empower Airmen leaders at all levels to effectively articulate and, in turn, comprehended Commander's Intent, and thereby distribute control, decentralize execution, and seize initiative at the lowest possible levels. Moreover, without a bolder approach to risk, Airmen will miss opportunities for initiative and innovation critical in future multi-domain, anti-access and area denial operations. To succeed in those future battlespaces, the Air Force must develop and entrust Airmen leaders to seek and exploit risk instead of fearing or completely avoiding risk, because the ability to expose, discover, and capitalize on unplanned but advantageous opportunities will be the decisive factor in future near-peer military conflict.

Shortfalls in Current Guidance

Joint Publication 3-0 describes RM as a "function of command and a key planning consideration,"[12]…a position fully congruent with the ISO definition of risk. However, the Joint guidance goes on to confuse "risk" with "frequency of occurrence", stating, "High-tempo operations may increase the risk of injury and death due to mishaps." Replace "risk" with "occurrence", and the meaning of the sentence remains the same.[13] The Air Force's recent update of AFI 90-802 "Risk Management" manifests a similar problem: it conflates hazard

analysis and mitigation with risk in general.[14] In addition to using "hazards" and "risks" interchangeably, the AFI limits risk to negative impacts and focuses on known threats versus uncertain events.

The confusion of terms goes further with the conflation of "hazard", "threat", and "risk" in commonly used decision guides across Air Force mission sets. Air Mobility Command's Threat Working Group guidance categorizes countries into tiers "according to the level of assessed risk to [Mobility Air Forces] operations".[15] The delineation of those "significant-moderate-low" risk tiers, however, is based on threats, not uncertainty.[16] This tiered approach to establish various minimum actions is appropriate and valid for dealing with known threats, but it does not address actual risk. Tactical operators use a similar approach, called Acceptable Level of Risk (ALR), which again is actually a means to dictate tactical action based on known threats. Figure 2 shows a familiar form of an ALR table from an article written for the F-15E Strike Eagle community. This table and many like it provide useful rules-of-thumb for young operators to make quick decisions based on the hazards they encounter. But this table is not about actual risk. Each "level" is tied to loss or potential losses based on historical trends. For example, the article defines "Medium Risk" as "Losses expected at historical combat rates," and "High Risk" as "Expected losses may render unit unfit for further combat."[17] Historical combat loss rates are essentially meaningless today, and almost certainly will be in the future. What combat loss rate should apply to stealth bombers, or to fifth-generation fighters? The loss of a single B-2 would cost billions of dollars. Does that constitute a "major loss"? How does the associated human toll compare to the loss of highly advanced weapons systems? In addition to addressing only known or anticipated threats, tying the definition of risk to loss, as both Joint and Air Force guidance do,

hampers senior leaders' ability to convey their intent with regard to initiative and innovation, and it inhibits subordinate commanders from seeking rational risk.

Table 2. Air-to-Ground Tactics Limits based on ALR		
Acceptable Level of Risk	**Definition**	**A/G Tactics**
NEGLIGIBLE	No losses acceptable.	Do not enter lethal WEZ of any SAM or AAA. Use medium/high altitude tactics only.
LOW	Accept only favorable engagements.	Do not enter lethal WEZ of AAA or MANPADS. Enter SAM WEZ only with fully effective SEAD.
MEDIUM	Accept neutral or disadvantageous engagements; Withdraw to preserve forces.	Enter AAA, MANPAD WEZs as required. Enter SAM WEZ with partially effective SEAD. No reattacks if being engaged.
HIGH	Accept major losses to achieve objective; Preserve some future capability, if able.	Enter S/A WEZs with marginally effective SEAD. Reattack as required but withdraw if threat overwhelming (e.g., suffer 25% losses).
EXTREME	Accept any losses necessary to accomplish mission.	Enter S/A WEZs without SEAD if required. Do not withdraw until target destroyed.

Figure 2. Example ALR Table.[18]

Addressing Risk Aversion

In addition to creating pressure to constantly minimize risk, thereby inadvertently minimizing opportunity, AFI 90-802 implements RM as a means to restrict authority from flowing down the chain of command and to apply pressure to relinquish decisions up the chain. This approach is antithetical to the goal of Operational Agility, and although the AFI mentions avoiding "risk aversion", it uses stark language enjoining Airmen to avoid decisions if there is any chance at all that a higher level "should" make that decision. It tells commanders, "The intent [of RM] is to ensure that as risk levels increase, risk acceptance and associated Go/No-Go decisions are elevated to obtain appropriate commander/supervisory oversight and approval." It goes on to state, "Leaders and individuals must be aware of how much risk they can accept and when to elevate [RM] decisions to a higher level."[19] The implications are clear: the presence of risk should be accompanied by the restriction of decision authority to ever-higher levels of the

chain of command. Yet the AFFOC states that Operational Agility requires Airmen who can make quick decisions and have the ability to act immediately on those decisions.[20] There are certainly reasonable limits on the types of decisions lower-level commanders can make, but those should be delineated in the operational limitations. A comprehensive Risk Profile, as described below, is the best tool to empower risk decisions within reasonable bounds.

Most damning of all is the AFI's description of the second RM Principle: "Make risk decisions at the appropriate level." Airmen are admonished that, "Those accountable for the success or failure of the mission or activity must be fully engaged in the risk decision process."[21] Again, this approach to risk is incompatible with Operational Agility, because it applies pressure for decision making in the wrong direction—up the chain of command. To empower Airmen to seize initiative, leaders who are accountable for the mission must have the courage to delegate risk decisions down the chain. To achieve Operational Agility, it is imperative that senior leaders, as the "risk owners", embolden their subordinate commanders to make risk decisions *on their behalf*. The Air Force's own vision of the future asserts that trust will be central to combat success[22], but this AFI indoctrinates decision avoidance and bakes in a lack of trust in lower-level commanders. Of note, the AFI's authors actually recognize that their approach to risk-based decision making is a recipe for failure when it really counts, by caveating the severe yet vague restriction on pushing authority down the chain of command: "Risk decisions must never be delegated to a lower level for convenience or when the situation dictates senior-level involvement; *exceptions may be considered in time critical situations where delays might endanger lives, resources or equipment* [emphasis added]."[23]

Why is such risk aversion the rule instead of the exception? After all, the Air Force was founded by bold risk-takers and innovators. It turns out risk aversion, as a concept, originated

alongside one of the roots of aviation itself. Daniel Bernoulli, the same Swiss mathematician famous for his equation used to calculate aerodynamic lift, also characterized risk aversion based on the asymmetry between human perceptions of loss and gain.[24] Bernoulli recognized and sought to describe the phenomenon wherein humans perceive that an incremental loss has a greater magnitude of value—what he coined as "utility"—than the value associated with an equal, albeit positive, incremental gain. Figure 3 depicts this phenomenon that can lead to poor risk decisions.[25]

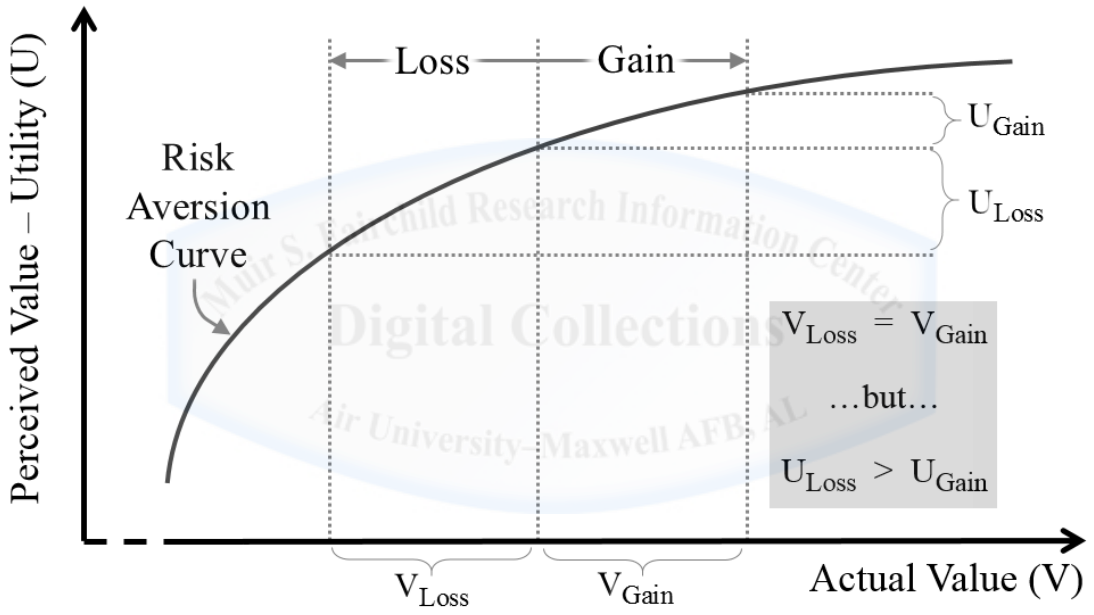

Figure 3. Risk Aversion Based on Actual versus Perceived Value

In addition to humans' natural risk aversion, Damodaran points out other factors that exacerbate this phenomenon. Risk aversion tends to increase with the magnitude of the stakes involved.[26] Humans are also notoriously bad at assessing the probabilities associated with complex scenarios[27], and emotion tends to cloud perceptions of risk.[28] Also, as the frequency of feedback on a given situation increases, aversion to loss actually intensifies, adversely impacting

risk decisions.[29] Mauboussin piles on concerning complex situations which involve both skill and luck. He points out that, when luck is involved, feedback is often misleading, because apparent cause and effect are poorly correlated.[30] Now picture a General in command of a large-scale military operation sitting in a command center watching real-time video from a drone or a body-cam of a small-team tactical mission. Combining what seems like a fine temporal granularity of situational awareness with such a high level of authority may seem attractive, since the General has broad decision-making powers to shape the scenario as it unfolds. Yet, this is the worst possible situation for risk aversion preempting sound decision making. The stakes are already high given the scope of the General's responsibilities to the operation at large. Viewing the mission through a soda-straw certainly does not enhance the General's ability to assess probabilities of future events facing the tactical team. And the frequency of feedback—in this case essentially infinite, i.e., continuous—is prone to be misleading as the element of luck influences the mission, even as it intensifies the General's aversion to loss. Damodaran and Mauboussin thus discredit the notion that higher-ranking commanders at increasing distances from the point of action will make better risk decisions than their subordinate commanders.

Adopting a New Definition of Risk

Various disciplines, such as finance and engineering, use different and equally valid descriptions of risk.[31] However, two common themes arise in most definitions.

- Risk pertains to present and future outcomes. Risk relates to events that have not yet occurred or that are in the process of unfolding, wherein the final outcome is as yet unknown. This theme is captured in the ISO definition's element of "uncertainty".[32]

- Risk is a function of perception and values.[33] Outcomes represent consequences of events, and different stakeholders may have widely varying views on the nature and magnitude of those consequences. This theme is captured in the ISO definition's elements of "effect" and "objectives".

The ISO's generalized definition is consistent with those well-vetted themes.[34] The JP 1-02 definition includes related themes but deviates from the ISO definition in two consequential ways. First, it omits "uncertainty" and uses "probability". The international standard purposely avoids the use of "probability" in the basic definition of risk specifically because, at least in English, probability is "often narrowly interpreted as a mathematical term."[35] The ISO recognizes that risk is often not mathematically quantifiable and opts for the term "likelihood" to cover both qualitative and quantitative characterizations of risk. The Joint definition misses that key insight about the qualitative side of risk. But more importantly, risk is intrinsically coupled with the broader notion of uncertainty. Air Force RM uses the product of expert opinions about the criticality and impact of known or anticipated hazards[36], effectively masking the underlying uncertainty. As a result, most references to "Risk Management" in Joint and Air Force guidance represent a misnomer. The processes they describe could instead be titled "Resource Allocation for Hazard Mitigation" or "Hazard Thresholds for Initiating and Continuing Operations", because they only address down-side risk mitigation (i.e., risk hedging[37]). Those mislabeled processes may be useful, but they do not sufficiently address risk as a whole, and, as written, they inhibit the up-side of risk which should empower Airmen to seek out and exploit risk in order to discover and take advantage of previously unavailable opportunities.

Therein lies the second important difference between the ISO and Joint definitions of risk: JP 1-02 limits the scope of risk to negative consequences, i.e., "loss". The international

standard definition of risk includes the potential for positive or beneficial consequences in addition to the more common uses of risk referring to negative impacts. The Joint definition hampers initiative by emphasizing that risk is intrinsically negative and fraught with the potential for harm, and therefore should always be minimized. Damodaran argues the best approach to risk includes the potential for both negative and positive outcomes, and that focusing on minimizing risk "will also reduce the potential for opportunity."[38] Although Damodaran wrote primarily for investors, this is a crucial insight for military leaders. By defining risk in purely negative terms and inducing pressure to constantly reduce risk, all with the understandable purpose to eliminate mishaps and undesired outcomes, joint doctrine and Air Force guidance also inadvertently minimize opportunities.

By adopting the ISO definition, Joint and Air Force guidance can align with Industry's collective wisdom and set the foundation to pivot leaders from a negative to a positive orientation toward risk, because an "effect" can be beneficial or harmful. By using "uncertainty" instead of "probability", the new definition adheres to Damodaran's enjoinder that risk must encompass both objective and subjective uncertainty[39], because the complexity of military operations makes it impractical or impossible to calculate valid probabilities pertaining to most decisions that matter in strategy and combat. In addition, by tying risk to "objectives", military leaders can better quantify and communicate their risk profiles—aggregations of specific risks and associated exploitation and hedging measures[40]—as part of Commander's Intent, a crucial enabler for decentralization of military decision making.[41] Figure 4 provides proposals for new definitions to disambiguate risk and its key elements from other related but separate concepts, and to provide commanders a foundation for making and decentralizing risk decisions.[42]

Term	Proposed Definition for Joint and U.S. Air Force Doctrine
Risk	effect of uncertainty on objectives (expressed as a combination of events, consequences, and likelihoods, and the uncertainty associated with any or all of those factors)
Uncertainty	the state of (complete or partial) deficiency of information, knowledge, or understanding
Exposure	the state in which a consequence—negative or positive—that affects an objective may be realized (to any non-trivial degree)
Opportunity	exposure to expedients which impart beneficial effects on objectives
Danger	exposure to hazards which impart harmful effects on objectives
- The definition of "Risk" and its expression is taken directly from ISO 31000:2009(E) which also references ISO Guide 73:2009, *Risk Management - Vocabulary*. - The current Joint Publication 1-02 definitions of "effect" and "objective" are congruent with the ISO definitions of those terms and are sufficient for use with this new definition of "Risk" for Joint doctrine. - The definition of "Uncertainty" is adapted from ISO 31000:2009(E). - The definition of "Exposure" is adapted from Holton's discussion thereof: "A self-conscious being is *exposed* to a proposition if the being would care whether or not the proposition is true. The word *would* is critical to this definition. It is possible to be exposed to a proposition without knowing of or considering the proposition." Holton describes the link between Risk and Exposure as: "Risk, then, is exposure to a proposition of which one is uncertain."	

Figure 4. New Definitions for Risk and Related Terms

Applying the New Definition

One of the most important military manifestations of risk is in the Course of Action (COA) selection process. The description of hazards often acts as a proxy for determining relative risk levels between each COA. The Joint definition of risk equates the greatest number and severity of hazards with the greatest risk. However, a key to understanding risk is the fact that even if COA option-A unambiguously involves fewer hazards than option-B, option-A may still involve significantly more *risk* than option-B. The fact that risk is intrinsically tied to uncertainty uncouples the notions of risk and hazard: risk and hazards are not necessarily correlated (although they often seem to be). This new, perhaps counterintuitive, concept of risk bears repeating from different angles. A COA that is "safer" than other COAs may simultaneously be "riskier" than some or all of those other COAs. The inverse is true as well: a

COA involving intense overlapping hazards may still involve less risk than other options. Appendix A provides a potential future scenario that delves into the nature of the ISO definition of risk and disambiguates it from hazard assessment.

Pivoting to a Positive Risk Orientation

Once risk is decoupled from hazards and loss, such that risk can encompass both positive and negative outcomes, leaders can choose their approach, whether from a negative or risk-averse orientation, some kind of balanced approach, or a positive orientation that values risk-exploitation. In a 2013 paper published by the Joint Staff J7 titled "Mission Command and Cross-Domain Synergy", General (Retired) Gary Luck asserts a common view of modern combat operations, that "Today's interconnected world is unpredictable and complex", and that, in order to function at "the speed of the problem", commanders must accept "becoming uncomfortably decentralized to achieve mission success".[43] The J7 paper stops short of advocating for decentralized risk exploitation even as it emphasizes other aspects of empowerment and delegation. However, the combined insights of Damodaran and Mauboussin indicate that a positive orientation to risk with decentralized risk exploitation is more likely to lead to success in the complex military operations anticipated the Joint Staff.

Combat operations over the last twenty years might precipitate an illusion that the U.S. military's superior skill is and will continue to be the decisive factor in combat success. However, neither the Joint Operating Environment 2035 nor the Air Force Future Operating Concept envision that vastly asymmetric advantage persisting in all future scenarios.[44] While American service members may retain superiority in skill, determination, and discipline over potential adversaries, the emergence of near-peer competitors will diminish the benefit of that

superiority, i.e., the Paradox of Skill will manifest in near-peer combat. While one cannot control luck (anything subject to control necessarily falls in the category of skill), it is possible to open up availability of expedients that luck may create by empowering commanders at the point of action to make real-time decisions about exposure.

Mauboussin describes several phenomena that, in combination with the Paradox of Skill, make decentralized risk exploitation advantageous. First, for rapidly changing environments, strategies that incorporate exploration and experimentation are more likely to succeed than those that seek previously-"reliable" near-term successes.[45] Second, according to previous studies about established corporations and up-starts, disruptive innovation requires autonomy.[46] Large, centralized companies attempting to execute ground-breaking innovation tend to fail. If innovation and the ability to seize the initiative with new and creative solutions is necessary, then U.S. military leaders must push as much autonomy as possible down the chain of command and encourage an experimentation mindset, where failures are valued as opportunities to learn and adapt. Third, in contests between strong and weak opponents involving luck and skill, the strong opponent should seek to simplify the engagements in order for their superior skill to create the maximum advantage. The weak opponent, on the other hand should complicate the engagements so that luck has a greater influence on the outcome.[47] In future near-peer conflict, no amount of simplification will make an only-marginal advantage in skill decisive. In that case, U.S. commanders will have a choice to either continue as though they are the stronger opponent, leaving the outcome against a near-peer opponent essentially up to luck (again due to the Paradox of Skill), or to pivot to a weak-opponent's strategy to capitalize on *both* luck and skill.

By decentralizing risk exploitation decisions, commanders can effectively complicate the engagements by creating many smaller contests for decision superiority instead of a few large

centralized clashes between high-level decision makers. With commanders empowered at the point of action, U.S. forces can then turn a marginal advantage in the skill of command decision making into a decisive advantage. According to Mauboussin, the more chances there are to "score", the more skill will play a role in the aggregate outcome.[48] Decentralized risk exploitation will create hundreds, if not thousands of chances for U.S. commanders to "score" with decision superiority by autonomously exploiting—via innovation—the opportunities made available through complicating the contest in the first place. Each delegation of a risk decision certainly costs senior leaders—they must absorb the consequences if a lower-level commander's decision results in failure. But, by empowering those decisions to the lowest level, i.e., paying the cost for investing in multiple decision superiority engagements, senior commanders actually make severe negative outcomes less probable, and decisive positive outcomes more likely.[49] Mauboussin also reminds his readers that risk takers may achieve high or low returns, but risk aversion only leads to average results.[50] It seems clear that military operations against a near-peer adversary will not be won through a series of engagements where the results are "average".

A New Approach – Start with Risk Exploitation

The following two-step approach complements existing Joint and Air Force RM processes by adding additional uncertainty-based risk assessments to the planning process, as well as "baking in" risk exploitation to selected COAs, and by providing a means to communicate commanders' risk profiles which guide risk exploitation during execution.

COA COMPARISON

Instead of attempting to quantify total risk per COA (an essentially impossible task for complex military operations), a better approach is to assess the difference in positive and negative risks between COAs. Note that risk is rarely symmetrical[51]; there is almost always greater down-side than up-side risk associated with any activity, and combat is no exception. In general, there are far more ways a mission, operation, or campaign can go wrong that it can go right. For this reason, planners should start analysis of risk with considerations of the up-side, so as not to become buried in the down-side assessments such that the potential for opportunity becomes a terse afterthought. In a side-by-side comparison of risks associated with each COA, planners should "factor out" risks that are common or similar between COAs. That does not mean the risks are unimportant, they are just not compelling in the COA comparison process. Planners can then show commanders the difference between the number and type of unique risks encompassed by each COA. In addition, planners can use the techniques in Appendix B to further refine their COA selection process: comparison of success and failure modes, and comparison of assumptions.

COMMANDER'S INTENT – The Risk Exploitation Profile

Because most of the Operational Environments Airmen will encounter are constantly changing, even a COA that best exploits available up-side risk will begin to degrade in effectiveness from the moment the final draft is complete. Therefore, in addition to selecting COAs that optimize opportunities, Commanders must provide guidance such that lower-level decision makers seek and respond to risk with the same mindset as their senior leaders. This is not to say that lower-level leaders will or must always make exactly the same decisions that their

higher-level commanders would in a given situation. Effective implementation of Mission Command requires strong senior-level leadership, and that strength is a function of how well they can adapt to and incorporate subordinates' rational and reasonable decisions, even if those decisions are different from what the senior-level leaders would themselves have chosen. Instead of trying to anticipate every decision point and dictating the "right choices", the best way to enable subordinate decisions that are concordant with the senior commander's intent is to use risk to guide those decisions within the hard boundaries set by operational limitations. Subordinates, therefore, need some rubric to gain an understanding of their Commander's Risk Profile. A commander's risk profile should be positively oriented towards risk, i.e., it should encourage seeking opportunities and seizing initiative, as the example in Figure 5 depicts.

(Sample) **Risk Profile as Part of Commander's Intent**				
Based on your Situational Awareness (SA), your assessment of the uncertainty within your SA, & your command judgment, I expect you to seek rational risk that is Nominal, Elevated, Substantial, or Maximal, in accordance with the profile below, in order to reveal or create pivotal opportunities & in order to seize initiative to best accomplish the operation's objectives.				
In order to reveal or create Opportunities that… →	Advance Objective Accomplishment Further* than Planned Action (*better than a marginal improvement)	Turn operation from losing or neutral to winning or that Complete an Objective advantageously early	Achieve Decisive Victory or Simultaneously Complete multiple Objectives advantageously early	Preserve Large-scale Force Survival
Regarding Specific Objectives… →	Target Sets: G-…-A Or AOD Priorities X-or-Higher	Target Sets: D-…-A or AOD Priorities Y-or-Higher	Target Sets: A-B-C or AOD Priorities Z-or-Higher	Prevent or mitigate catastrophic OE down-turn
	Note: Objective value / criticality *increases* from Nominal to Maximal →			
Seek Risk that is →	**Nominal**	**Elevated**	**Substantial**	**Maximal**
Deviate from planned task when the Operational Environment (OE) worst case such that…	Deviation is similar to an existing branch plan, IPOE is complete & valid, & the OE has not shifted significantly from the state in which that branch plan was written	Deviation is dissimilar from any branch plan, however, IPOE is complete & valid, & the OE has not shifted significantly from the state in which the original mission was tasked	Deviation is similar to an existing branch plan, however IPOE is incomplete or unavailable, & the OE may have shifted significantly	Deviation is unplanned, IPOE is incomplete or unavailable, & the OE has shifted significantly
…And when you assess maximum likely Consequences of Execution such that…	2nd- & 3rd-order effects are well understood	2nd- & 3rd-order effects roughly equivalent to planned missions are anticipated with *low* susceptibility to knock-on effects	2nd- & 3rd-order effects roughly equivalent to planned missions are anticipated with *high* susceptibility to knock-on effects	2nd- & 3rd-order effects are unknown
When deviating from assigned tasks to pursue risk & opportunity, I expect you to optimize integration with other forces and missions and force packaging with available resources & to conduct rational hazard mitigation. In addition, the following lowest-levels-of-support apply to each category of risk.				
Minimum Tactical C2 capacity	Tactical C2 assets & capacity available to be assigned to the new mission	Tactical C2 assets & capacity must be shared / divided among existing tasks	Tactical C2 is ad hoc or a non-C2 agency is performing C2 functions	No available supporting Tactical C2
Minimum ISR / Sensor Coverage	Available ISR & sensor coverage is equivalent to planned mission(s.	ISR & sensor coverage must be shared / divided between new mission & other on-going missions	ISR is ad hoc or a non-traditional agency is performing ISR	No available supporting ISR
How to read this table…Example = Elevated Risk, paraphrased as: "In order to reveal opportunities that convert a situation where friendly forces are losing (or neutral) to winning, I expect you seek and exploit elevated risk. Such risk exploitation may result in an unplanned deviation, however, do not proceed with such deviations without a valid Intelligence Preparation of the Operational Environment (IPOE) or if the Operational Environment (OE) has evolved significantly since your original tasking was planned. Deviations with elevated risk should still have Tactical C2 and ISR support, although dedicated support is not required."				

Figure 5. Example Risk Profile: Senior Commander guidance for Subordinate Leaders

Recommendations

In order to pivot the Air Force to a positive risk orientation that empowers commanders at all levels with decentralized risk exploitation, the Air Force should adopt the definitions for risk and associated terms given in Figure 4. The Air Force should also augment the JOPP with the COA comparison and Commander's Risk Profile processes described above and in Appendix B. If those changes prove valid and beneficial, the new definitions and risk assessment processes should be considered for incorporation into Joint doctrine and the JOPP.

Conclusion

The concept of Mission Command—touted as the foundation for decentralized execution in Joint doctrine[52], and as the underpinning of future multi-domain combat according to the Air Force Future Operating Concept[53]—identifies risk, specifically the acceptance of prudent risk, as one of its six principles[54], and as a component of "understanding"—a key attribute of effective military commanders.[55] Air Force and Joint leaders clearly believe that dealing with risk is intertwined with the exercise of successful command and with seizing initiative.[56] Industry recognizes that effective RM must include both risk hedging and risk exploitation. The U.S. Air Force must embrace the upside of risk whether a confrontation with a true near-peer adversary is imminent or not. Mauboussin describes an historical study of wars where the stronger opponent had at least a ten-to-one advantage over the weaker opponent. Incredibly, even with an order-of-magnitude advantage or more, the stronger nations only prevailed 72% of the time.[57] He concludes that nations which fail to pivot their strategies are likely to fail despite their advantages in strength or skill. The U.S. Air Force must pivot away from a negatively-oriented risk posture that applies insidious pressure to centralize decision making. Inasmuch as the best

defense is a good offense, the best approach to risk is one that exploits it, and the most powerful "risk management" measure is an Airman empowered to seek and capitalize on opportunities, without unnecessary delays, at the point of action.

APPENDIX A – Future Risk Decision Scenario

A Joint Task Force commander weighs two available options for temporarily degrading a terrorist organization's strategic communications capability as part of a larger campaign in the region. The terrorists use a digital film production facility in an unaligned country to create high-quality propaganda. Civilians comprise the majority of the facility staff, and the company creates commercials for legitimate businesses in addition to their off-the-books support for the terrorists. On some nights, a contract cleaning crew enters the otherwise unstaffed facility, although the schedule is random. The terrorist organization has coopted local military forces. As such, the studio falls within the protective coverage of the local military's 5th-generation Surface-to-Air Missile (SAM) systems and interceptor aircraft, all of which have been extensively analyzed by U.S. intelligence. The unaligned country has advanced early warning and electronic warfare assets capable of denying satellite navigation guidance for munitions and control channels for remotely piloted aircraft. Although the unaligned nation would not deliberately initiate attacks on U.S. forces—in the past the country has tolerated U.S. counter-terrorism strikes within their borders—intelligence analysts assess that the terrorists' current level of influence would trigger a lethal defensive response from the country's military commanders before political leaders could step in to reassert control. The objective is operationally limited by the requirements to minimize civilian casualties and to avoid a strategic loss by pushing the unaligned country into the sphere of other regional powers acting in opposition to the United States. The two COAs (which are mutually exclusive due to time constraints) are summarized as follows:

COA "Kinetic Strike" (COA-K): This option centers on human-in-the-loop guided munitions delivered by a single advanced stealth bomber escorted by three 5th-generation

fighters suppressing area-denial forces in the vicinity of the target. An extensively prepared network attack, supported by naval assets and other fighter aircraft executing a previously rehearsed diversion, creates a corridor through the country's coopted anti-access defenses for the strike package and the tanker which must tow the fighters within the corridor to provide sufficient time-on-station for their escort mission. U.S. cyber forces have already penetrated the unaligned country's military network, however, the forces creating the initial corridor would be barely above parity capability-wise against the formidable SAMs and resilient command and control (C2) architecture clustered along the country's borders. Once in country, the bomber's munitions have an ~85% chance of successful kinetic effects against the film production facility, and targeteers assess that there are no significant concerns about collateral damage due to the facility's isolation from other structures, although there could still be retaliatory fires against the strike package as they egress.

COA "Cyber Strike" (COA-C): This option uses no kinetic forces and relies solely on a different, recently developed cyber-attack technique affecting the studio facility directly. The film production servers are well protected by network security, but the building's central heating and cooling system is susceptible to a recently discovered vulnerability in its commercial control unit for which the local vendor has not yet provided a patch. U.S. cyber operators believe they can gain access to the country's civilian network to inject code that exploits the new vulnerability and causes unpatched control units to overheat the facility past the point necessary to permanently disable the film production computers and servers. Due to the technique's recent development and rapid deployment, cyber operators would be unable to hide its origin and attribution from a forensic analysis. Once successfully resident in the control units, the injected

code has an ~85% chance of disabling the computers and servers, and if it does, the heating-cooling systems themselves will also likely ignite, damaging or destroying the facility.

Which of these represents a "higher-risk" COA? Using the current JP 1-02 definition of risk, COA-K is clearly more risky. Military risk is often segmented into "Risk-to-Forces", "Risk-to-Mission"[58], and occasionally "Risk-of-Escalation" among others. The feint necessary to create the initial corridor entails the possibility of U.S. aircrews getting shot down. The pilots of the bomber and escort fighters must operate for longer periods of exposure to even more lethal weapons systems. COA-C involves no such "Risk-to-Forces". The "Risk-to-Mission" appears roughly equal, wherein both rely on initially gaining access, albeit in different domains, and the probability of success of both specific effects is ~85% once delivered. If both COAs were to proceed at night, the first-order possibility of civilian casualties is roughly equal, whether the cleaning crew happens to be present and subject to bomb-blasts or fire. Finally, COA-K seems to carry a far greater "Risk-of-Escalation" with an outright aerial invasion of the country's territory. So, according to Joint and Air Force guidance, the JTF planners could identify COA-C as the less-risky, and therefore "best" option. But does their recommendation represent a complete comparison between the two COAs?

Applying the ISO definition of risk to the scenario above paints a completely different picture of the relative risk between the COAs. Instead of looking at the hazards present or absent in the COAs, look for the unknowns. COA-K involves a thoroughly analyzed operational environment, with rehearsed tactics, well-understood asset-to-threat parings and collateral damage assessments, and at least the precedent of the foreign government's tolerance for U.S. military action within its borders. COA-C, on the other hand, involves a new technique on a recently revealed weakness. Will the malicious code propagate through the civilian network as

desired? Could the cleaning crew somehow stop the malfunction or otherwise intervene? Could other buildings experience the same effects, including the potential for a catastrophic fire? How will the foreign government respond if a U.S. military cyber attack were to be uncovered as causal in multiple building fires involving civilian deaths? COA-K certainly involves more hazards, far more when it comes to U.S. service members' lives, but COA-C is rife with uncertainty. That relatively greater volume of uncertainty coupled with the potential consequences associated with mission failure and strategic loss means that COA-C is actually the higher-risk choice—down-side risk in particular—*for the stated objective*, i.e., to temporarily degrade the terrorist's strategic communications without inducing strategic setbacks. COA-K is not risk-free. However, the operators present throughout each stage of the mission can respond and adapt to unforeseen circumstances in ways that the computer virus in COA-C cannot.

No formula or look-up table can tell commanders whether it is better to face the hazards of COA-K or to take the risk of COA-C. They must use their command judgment to weigh the criticality of the objective, the dependence of the larger campaign on achieving that objective, and the consequences of failing to achieve both the objective and overall goals of the campaign. Without a clear-eyed understanding that the "safer" COA (COA-C) is actually riskier, the commander could blindly choose the cyber-only option, believing that the only significant difference is the fact that COA-K puts Americans in immediate peril and COA-C does not, i.e., COA-C ostensibly minimizes short-term Risk-to-Forces. However, crippling the terrorists' ability to dominate the narrative, even temporarily, may be deemed crucial and necessary for achieving strategic success. In that case, the lower-risk option, COA-K, with its accompanying possible costs of blood and treasure, may be the best, albeit difficult, choice. There is likely to be no clear answer as to whether placing Americans in jeopardy is "worth it" to increase the

likelihood of success or to reduce the potential for damaging tenuous relationships in the region. There may be additional up-side risk, i.e., opportunities, associated with COA-C that may offset the down-side risk. The commander must rely on judgment qualitatively informed by both hazard assessments and by risk comparisons.

APPENDIX B – Techniques for Comparison of Relative Risk between COAs

Compare Paths to Success and Failure Modes

The JOPP provides a means for determining most of the ways an operation can realistically succeed. The main sequence of actions along with anticipated branches represent the planners' delineation of all of the ways an operation may succeed, taking into account available resources and changes in the Operational Environment (OE). However, the branches are based primarily on enemy actions or a change in friendly capabilities.[59] Given COAs with developed branches, Airmen should then apply the following additional analysis to each COA:

1. What additional opportunities (beyond those identified in the branch plans) could enable, expedite, or enhance objective accomplishment? (These additional opportunities can originate from unlikely, infrequent, or "black-swan" events and phenomena.)
2. Of those additional opportunities, which ones does the COA permit or facilitate (without significantly deviating from the plans and branches)? Which opportunities does the COA impede or prevent?
3. What actions (i.e., deviations from the plans and branches) could Airmen take in order to open up the possibility that those additional opportunities will manifest?

After considering potential up-side risk, planners should then further analyze down-side risk.

In this context, a "failure mode" is simply a way that the end-state of an operation may manifest as a draw or defeat. Failure modes reflect general outcomes that are difficult to quantify. Examples of failure modes include: "Lack of minimum or critical assets in position at the intended time of execution", "Loss of critical information element necessary to trigger key action", or "Exhaustion of critical support resources prior to completion of operation". The

JOPP devotes a great deal of attention to the objects and events that could cause an operation to fail, i.e., the hazards, danger (i.e., exposure to hazards), and threats (i.e., hazards driven and exacerbated by malign intent). Airmen can complement those assessments by comparing the available failure modes for each COA, and by applying the same analysis to the enemy, i.e., "In what ways may the enemy fail to achieve *their* objectives?" As with risks, factor out identical or very similar failure modes, leaving a list of unique failure modes for each COA. Based on the example scenario above, COA-C and COA-K both have the available failure mode of "Inability to gain access to primary target". Even though COA-C seeks access via a network topography and COA-K seeks access via the air domain, this failure mode should be factored out. COA-C, however, has a unique failure mode of "On-site third-party intervention prevents successfully delivered fires from achieving their desired effects", i.e., the cleaning crew may prevent the heating system from overheating or catching fire by cutting the power. If the bomber crew effectively employs their munitions on the film production facility, the cleaning crew cannot stop the bombs from detonating.

When presenting COAs for a decision, planners can then convey the difference between COAs in terms of how many opportunities are incorporated (as branch plans), how flexible each COA is (i.e., how many and what type of additional non-branch plan opportunities the COA allows), and the relative weight of restriction that each COA imposes on initiative (i.e., how many and what type of additional opportunities the COA prevents). In addition to folding the failure mode analysis back into branch planning in order to identify potential mitigation measures, planners can present the results for commanders to see which, if any, of the COAs have a large number of unique failure modes compared to the others. This is a qualitative indicator that such a COA engenders a higher degree of risk than those without as many

available, unique failure modes. Focusing the same analysis on the adversary, planners can determine a unique list of enemy failure modes which each COA either directly capitalizes on or at least makes available. This is another indicator that the COA with the most available, unique enemy failure modes incorporates a greater degree of up-side risk (opportunities).

Compare Assumptions

An assumption effectively locks down a critical variable within COAs to one value or state such that the uncertainty associated with that variable is essentially ignored in order to advance the plan. This is why making assumptions is the most dangerous thing that planners must do. The uncertainty associated with that key variable still exists and will continue to affect the objective up to the point in execution where reality intervenes and realizes the variable as one unique value or state, which may or may not be the one the planners assumed. Assumptions must be well-constructed in accordance with JP 5-0, such that invalidating an assumption requires planners to alter or abandon the COA.[60] With the vetted lists of assumptions for each COA, begin the comparison of assumptions by eliminating common denominators. In other words, if several COAs have an identical or very similar assumption in common, then that assumption does not materially impact the difference in total volume of risk between those COAs. The result is a set of unique assumptions for each COA. Next categorize each assumption by the nature of the assumptions' uncertainty (i.e., the critical variables' possible states): binary, trinary, uniform distribution, discernable distribution, or random. Table 1 below describes those assumption uncertainty variable characterizations in more detail. Again, this is an empirical process separate from but complementary to the existing Joint and Air Force RM processes. The techniques herein borrow concepts from quantitative methods, but this approach

applies specifically to decisions for which quantitative analysis is either infeasible or unavailable.

Table 1. Characterization of the Variables Associated with Assumptions

Variable Type	Description	Example
Binary	Variable only has two significant possible values or states, e.g., 1/0, on/off, yes/no, present/absent, good/bad	By the time of execution, will the adversary have deployed one of their 5th-Gen SAMs to Base X? – Yes/No
Trinary	Variable only has three significant possible values or states, typically where two are opposites and the third is neutral or central between the others, e.g., -1/0/1, present/en route/absent, bad/neutral/good	After the initial cyber-attack, will the 5th-Gen SAM at Base X be operational, degraded, or non-operational?
Uniform Distribution	Variable may assume a range of values or states (continuous or discrete) with roughly equivalent likelihoods	To which of the prepared launch sites will the mobile surface-to-surface missile unit deploy?
Discernible Distribution	Variable may assume a range of values or states (continuous or discrete) such that a mean and variance based on likelihood can be estimated	Of each militant tactical fighting element, what percentage are child-soldiers?
Random	Variable may assume a range of values or states (continuous or discrete), but with no discernible pattern of likelihood	How many of each constellation of navigation satellites will be fully operational and within line-of-sight when the adversary attacks?

Notes

[1] In addition to my advisor, Col Samuelson, I would like to thank the following people for their assistance with this paper: COL Joshua Walker, Col Jeremiah Monk, Lt Col Kevin Beeker, Lt Col Lauren Byrd, Col Jon Rhone, Col Jeffrey York, Lt Col Keith McGuire, Lt Col Ricardo Camel, and Col Matthew Smith. I benefited from their insights multiple times over the period of writing this research report. Any errors in logic are my own.

[2] Joint Publication (JP) 5-0, *Joint Operation Planning*, 11 August 2011: p. IV-37.

[3] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 11 August 2011: p. 206.

[4] Holton, Glyn A. "Defining Risk" *Financial Analysist Journal*, 60,6 (November/December 2004): p. 22.

[5] Readers who point out that several people have survived such situations may append the scenario wherein the aircraft is flying 15,000 feet above a rocky swamp filled with brain-eating-amoeba and populated by hungry alligators, such that the ultimate outcome is no longer in question.

[6] Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: p. 7.

[7] Army Doctrine Publication (ADP) 6-0, *Mission Command*, Department of the Army, May 2012: p. 1.

[8] Mauboussin, Michael J. *The Success Equation: Untangling Skill and Luck in Business, Sports, and Investing*. Boston, MA: Harvard Business Review Press (2012): pp. 53-58.

[9] Figure produced by the author based on the description in Mauboussin, Michael J. *The Success Equation: Untangling Skill and Luck in Business, Sports, and Investing*. Boston, MA: Harvard Business Review Press (2012): pp. 53-58.

[10] International Standards Organization (ISO) 31000:2009(E), *Risk Management – Principles and guidelines*, International Standards Organization: Geneva, Switzerland (2009): p. 1.

[11] Air Force Future Operating Concept. *A View of the Air Force in 2035*, September 2015: p. 2.

[12] Joint Publication (JP) 3-0, *Joint Operations*, 11 August 2011: p. III-5. Joint and Air Force guidance, under the label of "Risk Management" (RM), describe techniques to accomplish necessary planning and decision making processes, but those techniques either insufficiently address the full scope of risk, or they are mislabeled, defining processes that are peripheral or antecedent to comprehensively dealing with risk. The JP1-02 definition lags the industry standard, while the Air Force approach—quantifying risk as an equation —actually addresses "hazards" more so than risk as a whole. AFI31-101 carries that doctrine further with the equation: current Air Force-defined "Risk" = Asset Criticality x (Threat x Vulnerability). Air Force guidance conflates "risk" and "hazards", but the two concepts are and must be separate and distinct for military operations. Air Force Instruction (AFI) 31-101, *Integrated Defense*, Change 3, 3 February 2016: p. 52.

[13] The JP 3-0 authors' intended meaning seemed to be: "An increase in the frequency of mishaps that lead to injury or death is often correlated with an increase in operations tempo." The point being that command action is necessary to de-correlate mishap occurrence from ops tempo increases. But risk is not just "probability of occurrence", nor is it always the mathematical product of "probability of occurrence" and "severity of loss", nor is it always tied to hazard exposure. Risk is the effect of uncertainty on objectives; the hazard-probability-severity case is a subset of the broader concept of uncertainty. This may seem like a subtle difference, but it is important for understanding risk and to avoid confusing risk with other valid but separate concepts.

[14] The instruction states, "…we must always include the experience, expertise and knowledge of experienced personnel to identify known hazards/risks and strategies to effectively mitigate risks for the specific mission, activity or task in both on- and off-duty situations." It continues with, "The assessment step involves the application of quantitative and/or qualitative measures to determine the probability and severity of negative effects that may result from exposure to hazards/risks..." It also adds, "Effective assessment requires the key elements of hazard/risk identification and understanding the negative effects associated with those hazards/risks." Air Force Instruction (AFI) 90-802, *Risk Management*, 8 March 2016: pp. 14, 15, and 20 respectively.

[15] Air Mobility Command Instruction (AMCI) 14-106, *Threat Working Group (TWG)*, Change 1, 23 April 2014: p. 7.

[16] Air Mobility Command Instruction (AMCI) 14-106, *Threat Working Group (TWG)*, Change 1, 23 April 2014: p. 8.

[17] Lt Col Mark Kelly. "Just Give Me the Guidance and I'll Give You the Tactics", *Flying Safety* 60, 4 (April 2004): p. 12.

[18] Lt Col Mark Kelly. "Just Give Me the Guidance and I'll Give You the Tactics", *Flying Safety* 60, 4 (April 2004): p. 12. Physical hazards and threats to military operations—Enemy Order of Battle, meteorological phenomena, equipment and technology reliability—are typically well-defined and exhaustively analyzed. Familiar hazards to air, space, and cyber operations have observable and measurable characteristics with capabilities describable in terms of probabilities. An adversary SAM system has a maximum range and altitude, missile speed and maneuverability, guidance and sensors, warhead characteristics, infrared signatures, nation-dependent tactics, communications, command and control architectures, and so on. Airmen draw large red circles on charts representing lethal ranges of fourth- and fifth-generation SAMs and assume that the area inside those circles represents a region of high risk. But in fact most located SAMs—those that are not brand new or emerging technology such that there is still limited intelligence on them—do not significantly increase operational risk. Those systems absolutely pose a grave threat to Airmen and their aircraft and weapons, but a SAM with well-understood characteristics and a confirmed location or operating area does not impose a high degree of uncertainty. This is the tactical corollary of the skydiver-with-no-parachute.

[19] Air Force Instruction (AFI) 90-802, *Risk Management*, 8 March 2016: p. 20.

[20] Air Force Future Operating Concept. *A View of the Air Force in 2035*, September 2015: p. 7.

[21] Air Force Instruction (AFI) 90-802, *Risk Management*, 8 March 2016: p. 12.

[22] Air Force Future Operating Concept. *A View of the Air Force in 2035*, September 2015: p. 12.

[23] Air Force Instruction (AFI) 90-802, *Risk Management*, 8 March 2016: p. 17.

[24] Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: p. 13.

[25] Author produced this graphic based on the descriptions in Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: pp. 35-38.

[26] Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: pp. 61-63.

[27] Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: p. 63.

[28] Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: pp. 46-47.

[29] Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: p. 45.

[30] Mauboussin, Michael J. *The Success Equation: Untangling Skill and Luck in Business, Sports, and Investing*. Boston, MA: Harvard Business Review Press (2012): p. 27.

[31] Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: p. 6.

[32] International Standards Organization (ISO) 31000:2009(E), *Risk Management – Principles and guidelines*, International Standards Organization: Geneva, Switzerland (2009): p. 7.

[33] International Standards Organization (ISO) 31000:2009(E), *Risk Management – Principles and guidelines*, International Standards Organization: Geneva, Switzerland (2009): p. v.

[34] International Standards Organization (ISO) 31000:2009(E), *Risk Management – Principles and guidelines*, International Standards Organization: Geneva, Switzerland (2009): pp. 1-2. "risk…effect of uncertainty on objectives…NOTE 1 An effect is a deviation from the expected – positive and/or negative. NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). NOTE 3 Risk is often characterized by reference to potential events…and consequences…or a combination of these. NOTE 4 Risk is often expressed in terms of a combination of consequences of an event (including changes in circumstances) and the associated likelihood…of occurrence. NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence or likelihood.

[35] International Standards Organization (ISO) 31000:2009(E), *Risk Management – Principles and guidelines*, International Standards Organization: Geneva, Switzerland (2009): p. 5.

[36] Air Force Instruction (AFI) 90-802, *Risk Management*, 8 March 2016: p. 16.

[37] Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: p. 8.

[38] Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: p. 5.

[39] Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: p. 5.

[40] International Standards Organization (ISO) 31000:2009(E), *Risk Management – Principles and guidelines*, International Standards Organization: Geneva, Switzerland (2009): p. 5.
[41] Army Doctrine Publication (ADP) 6-0, *Mission Command*, Department of the Army, May 2012: pp. 3-4.
[42] The definitions for Figure 4 are derived from a combination of the following sources:
- International Standards Organization (ISO) 31000:2009(E), *Risk Management – Principles and guidelines*, International Standards Organization: Geneva, Switzerland (2009).
- Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 11 August 2011.
- Holton, Glyn A. "Defining Risk" *Financial Analysist Journal*, 60,6 (November/December 2004).

[43] General (Retired) Gary Luck, Insights and Best Practices Paper, *Mission Command and Cross-Domain Synergy*, Joint Staff J7, March 2013: pp. i, 1, and 9, respectively.
[44] The complexity of future combat and the likelihood of facing a near-peer adversary are themes throughout both the JOE 2035 (Joint Operating Environment - 2035. *The Joint Force in a Contested and Disordered World*, 14 July 2016.) and the AFFOC (Air Force Future Operating Concept. *A View of the Air Force in 2035*, September 2015.)
[45] Mauboussin, Michael J. *The Success Equation: Untangling Skill and Luck in Business, Sports, and Investing*. Boston, MA: Harvard Business Review Press (2012): p. 107.
[46] Mauboussin, Michael J. *The Success Equation: Untangling Skill and Luck in Business, Sports, and Investing*. Boston, MA: Harvard Business Review Press (2012): p. 184.
[47] Mauboussin, Michael J. *The Success Equation: Untangling Skill and Luck in Business, Sports, and Investing*. Boston, MA: Harvard Business Review Press (2012): p. 182.
[48] Mauboussin, Michael J. *The Success Equation: Untangling Skill and Luck in Business, Sports, and Investing*. Boston, MA: Harvard Business Review Press (2012): p. 181.
[49] Mauboussin extends the argument concerning the difference between "put" and "call" strategies in a complex environment as described in Taleb, Nassim Nicholas. "Antifragility, Robustness, and Fragility Inside the 'Black Swan' Domain" SSRN working paper, February 2011 (as cited in Mauboussin, Michael J. *The Success Equation: Untangling Skill and Luck in Business, Sports, and Investing*. Boston, MA: Harvard Business Review Press (2012): pp. 190-196.)
[50] Mauboussin, Michael J. *The Success Equation: Untangling Skill and Luck in Business, Sports, and Investing*. Boston, MA: Harvard Business Review Press (2012): p. 40.
[51] Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007: p. 27.
[52] Joint Publication (JP) 3-0, *Joint Operations*, 11 August 2011: p. II-2.
[53] Air Force Future Operating Concept. *A View of the Air Force in 2035*, September 2015: p. 10.
[54] Army Doctrine Publication (ADP) 6-0, *Mission Command*, Department of the Army, May 2012: pp. 3-4.
[55] General Martin E. Dempsey, *Mission Command White Paper*, 3 April 2012, p. 5.
[56] Joint Publication (JP) 5-0, *Joint Operation Planning*, 11 August 2011: p. I-2.
[57] Mauboussin references the study of conflict between 1800 and 2003 in Arreguín-Toft, Ivan. *How the Weak Win Wars*, Cambridge, U.K.: Cambridge University Press (2005), cited in Mauboussin, Michael J. *The Success Equation: Untangling Skill and Luck in Business, Sports, and Investing*. Boston, MA: Harvard Business Review Press (2012): pp. 185-186.
[58] Joint Publication (JP) 5-0, *Joint Operation Planning*, 11 August 2011: p. IV-39.
[59] Joint Publication (JP) 5-0, *Joint Operation Planning*, 11 August 2011: p. III-37.
[60] Joint Publication (JP) 5-0, *Joint Operation Planning*, 11 August 2011: p. A-4.

Bibliography

Air Force Future Operating Concept. *A View of the Air Force in 2035*, September 2015.

Air Force Instruction (AFI) 31-101, *Integrated Defense*, Change 3, 3 February 2016.

Air Force Instruction (AFI) 90-802, *Risk Management*, 8 March 2016.

Air Mobility Command Instruction (AMCI) 14-106, *Threat Working Group (TWG)*, Change 1, 23 April 2014.

Army Doctrine Publication (ADP) 6-0, *Mission Command*, Department of the Army, May 2012.

Damodaran, Aswath. *Strategic Risk Taking: a Framework for Risk Management.* Upper Saddle River, NJ: Pearson Education Inc., 2007.

Dempsey, General Martin E. "Mission Command White Paper", 3 April 2012.

Holton, Glyn A. "Defining Risk" *Financial Analysist Journal*, 60,6 (November/December 2004): p. 19-25.

International Standards Organization (ISO) 31000:2009(E), *Risk Management – Principles and guidelines*, International Standards Organization: Geneva, Switzerland (2009).

Joint Operating Environment - 2035. *The Joint Force in a Contested and Disordered World*, 14 July 2016.

Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 11 August 2011.

Joint Publication (JP) 3-0, *Joint Operations*, 11 August 2011.

Joint Publication (JP) 5-0, *Joint Operation Planning*, 11 August 2011.

Lt Col Mark Kelly. "Just Give Me the Guidance and I'll Give You the Tactics", *Flying Safety* 60, 4 (April 2004): pp. 10-15.

General (Retired) Gary Luck, Insights and Best Practices Paper, *Mission Command and Cross-Domain Synergy*, Joint Staff J7, March 2013.

Mauboussin, Michael J. *The Success Equation: Untangling Skill and Luck in Business, Sports, and Investing*. Boston, MA: Harvard Business Review Press (2012).